

# SANA

## Network Security through artificial Immunity

Research Day MINE-Group  
July 2007

Michael Hilker  
email: [michael.hilker@uni.lu](mailto:michael.hilker@uni.lu), phone: +352-466644-5415

# SANA

- The artificial immune system SANA is a framework to implement a distributed security system. It provides a library of non-standard approaches for security components enhanced with common-used components. The organisation and the information management is more sophisticated for lots of collaboration between the components.
- The architecture is fully distributed with self-organising artificial cells performing the required tasks for network security.
- Cooperative work is used in order to implement novel features and to detect suspicious behaviour.

# Overview SANA

# Overview SANA

- Security environment

# Overview SANA

- Security environment
  - Artificial cells

# Overview SANA

- Security environment
  - Artificial cells
  - Security components

# Overview SANA

- Security environment
  - Artificial cells
  - Security components
- Artificial cell communication

# Overview SANA

- Security environment
  - Artificial cells
  - Security components
- Artificial cell communication
- Self management

# Overview SANA

- Security environment
  - Artificial cells
  - Security components
- Artificial cell communication
- Self management
- Information Management

# Overview SANA

- Security environment
  - Artificial cells
  - Security components
- Artificial cell communication
- Self management
- Information Management
- Cooperative workflows

# Overview SANA

- Security environment
  - Artificial cells
  - Security components
- Artificial cell communication
- Self management
- Information Management
- Cooperative workflows
- Self-checking, -healing

# Overview SANA

- Security environment
  - Artificial cells
  - Security components
- Artificial cell communication
- Self management
- Information Management
- Cooperative workflows
- Self-checking, -healing
- Checking from outside

# Overview SANA

- Security environment
  - Artificial cells
  - Security components
- Artificial cell communication
- Self management
- Information Management
- Cooperative workflows
- Self-checking, -healing
- Checking from outside
- SOA for security environments and installed user systems

# Overview SANA

- Security environment
  - Artificial cells
  - Security components
- Artificial cell communication
- Self management
- Information Management
- Cooperative workflows
- Self-checking, -healing
- Checking from outside
- SOA for security environments and installed user systems
- Copy and halt of systems for further analysis and legal aspects

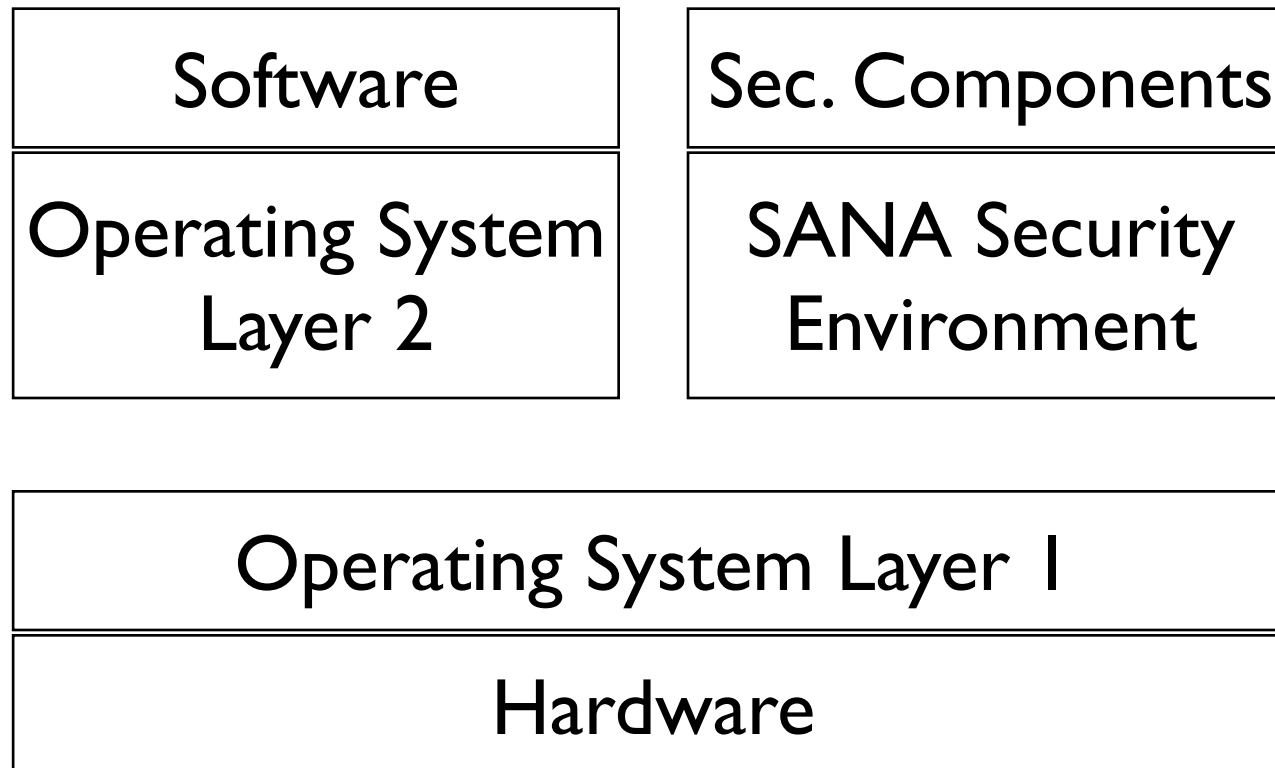
# Overview SANA

- Security environment
    - Artificial cells
    - Security components
  - Artificial cell communication
  - Self management
  - Information Management
  - Cooperative workflows
  - Self-checking, -healing
- Checking from outside
  - SOA for security environments and installed user systems
  - Copy and halt of systems for further analysis and legal aspects

# Distributed Systems

- Distributed Systems with mobile/roaming entities requiring some kind of environment in which the entities work.
- The environment is a middleware between the resources of the network node and the entities.
- It manages the access to the resources as well as the security in the access.

# Security Environment as Middleware for Cells



# SOA Architecture

- Operating system and security environment run in virtual machines and can be transferred over the network as well as halted and duplicated.
- The operating system as well as the security components are provided as service in a service oriented architecture (SOA)
- Components check the operating system from outside

# Advantages

- Other security components can be easily demanded and provided.
- A copy of the intrusion is stored for further analysis and legal aspects.
- Attacker have more problems to hide itself from checking.
- Production breakdown is reduced.

# Disadvantages

- Overhead of virtualisation (about 1-20 %)
- Some intrusions detect virtualisation and disable itself
- Virtualisation tools maybe not ready for deployment for such a system

# Security in the Implementation

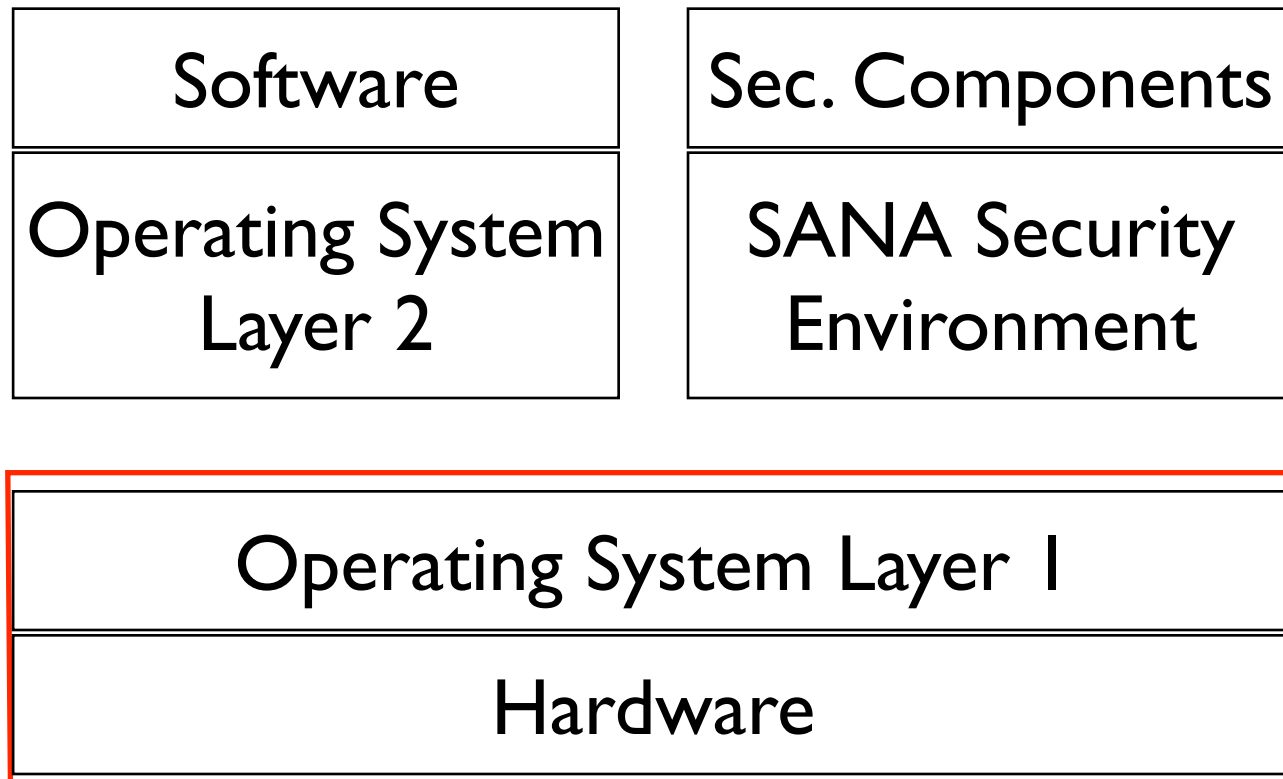
- Problem:

An intrusion installs itself in the node.

Does it receive access to the security system with its internal information?

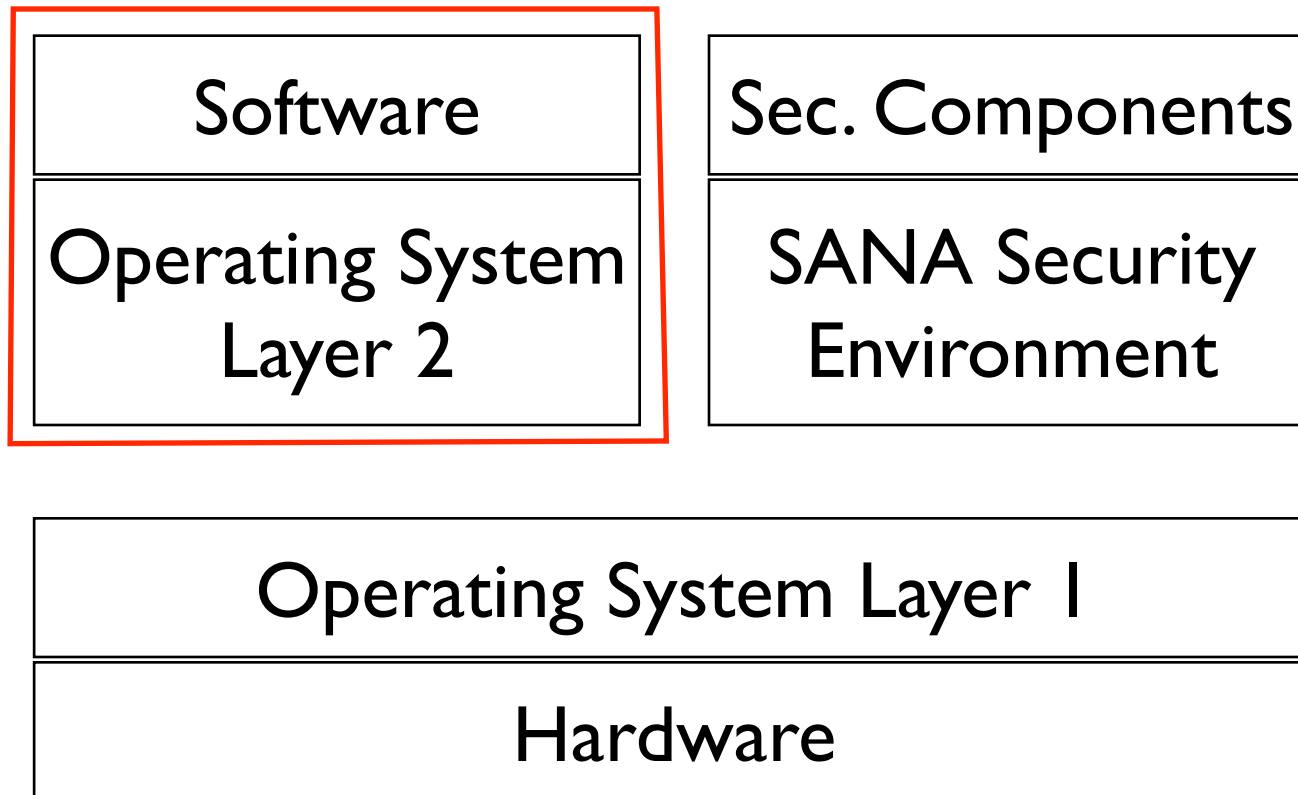
Can the intrusion use the security system for propagation?

# Intrusion in OS Layer I

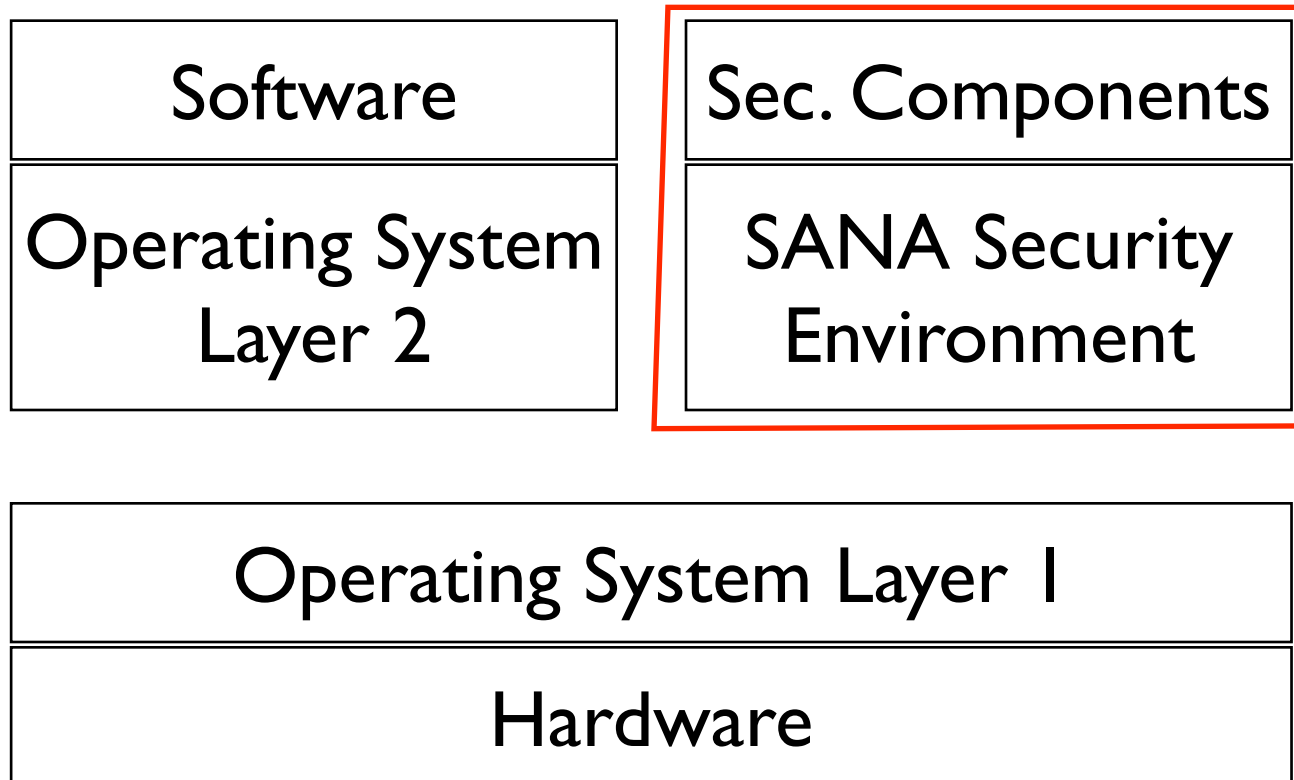


# Intrusion in OS Layer 2

## Application Software



# Intrusion in OS Layer 2 Security Software



# Activities

- Participation in the 3rd International Conference on Web Information Systems and Technologies (WEBIST 2007), Barcelona, Spain, March 2007 by C. Brucks and C. Wagner.
- Workshop Theory of Viruses 2007 (TCV 2007) in Nancy, France.
- 21st Conference on Computer, Electrical, and Systems Science, and Engineering (CESSE 2007) in Vienna, Austria. Invited to submit an extended version as journal article.

# Future Activities

- Software demonstration at the 6th International Conference on Artificial Immune Systems (ICARIS 2007), Santos/SP, Brazil in August 2007.
- Accepted paper at the 2nd International Conference on Bio-Inspired Computing: Theories and Applications (BIC-TA 2007), Zhengzhou, China in September 2007
- Journal article submitted to Journal on Computer Viruses (JCV) as an extended version of the TCV 2007 article; currently under review.
- Improve article about the artificial cell communication for a new conference in cooperation with Katja Luther from the DAI-Labor, TU Berlin, Germany.
- Journal article about ANIMA through CESSE 2007.

# Conclusion

- SANA is a distributed framework to secure a network against intrusions.
- Cooperative work increase the performance.
- SOA enables more fault-tolerant production in the network and enables features required for novel security systems.

# References

- M. Hilker: Distributed Self Management for Distributed Security Systems. Proceedings of the 2nd International Conference on Bio-Inspired Computing: Theories and Applications (BIC-TA 2007), September 2007, Zhengzhou, China. (to appear)
- B. Schroeder, M. Hilker, R. Weires: Dynamic Association Networks in Information Management. Proceedings of the 21st International Conference on Computer, Electrical, and Systems Science, and Engineering. (CESSE 2007), May 2007, Vienna, Austria.
- M. Hilker, C. Schommer: SANA - Network Protection through artificial Immunity. Proceedings of the 2nd International Workshop on Theory of Computer Viruses (TCV 2007), May 2007, Nancy, France.
- C. Brucks, C. Wagner, M. Hilker, R. Weires: CoZo - Content Zoning for Spam Email. Proceedings of the 3rd International Conference on Web Information Systems and Technologies (WEBIST 2007) March 2007, Barcelona, Spain.
- M. Hilker, C. Schommer: AGNOSCO – Identification of Infected Nodes with artificial Ant Colonies. Proceedings of the 6th International Conference on Recent Advances in Soft Computing (RASC2006) July 2006, Canterbury, United Kingdom.
- M. Hilker, C. Schommer: SANA – Security Analysis in Internet Traffic through Artificial Immune Systems. Proceedings of the Trustworthy Software Workshop, May 2006, Saarbruecken, Germany.
- M. Hilker, C. Schommer: Description of Bad-Signatures for Network Intrusion Detection. Proceedings, Fourth Australasian Information Security Workshop (AISW-NetSec 2006) during the Australasian Computer Science Week, Conferences in Research and Practice in Information Technology (CRPIT), Vol. 54, January 2006, Hobart, Australia.
- M. Hilker, C. Schommer: A new queueing strategy for the Adversarial Queueing Theory. Proceedings, IPSI-2005 December 2005, Bled, Slovenia.
- M. Hilker: Queueing Strategien im Internet Routing. Diploma Thesis at the JW Goethe-University, March 2005, Frankfurt/M., Germany.